Incident Response Planning

The 15 Minute Workgroup Tabletop Exercise

January 2016

Provided for your use is a 15-minute tabletop exercise template for use in developing education and awareness at your agency. These exercises are brought to you by the State Office of Cyber Security, Security Operations Center (SOC), with a mission of providing centralized information sharing, monitoring, and analysis of Washington State's security posture.

The goal of the tabletop exercise is to increase security situational awareness and to facilitate discussion of incident response in as simple a manner possible; targeting a time range of 15 minutes. The exercises provide an opportunity for management to present realistic scenarios to a workgroup for development of response processes.

How to best use the tabletop exercise:

1. Modify the tabletop scenario as needed to conform to your environment.

2. Engage management.

3. Present scenario to the workgroup.

4. Discuss the process to address the scenario.

5. Document the response and findings for future reference

Note: A member of the State Office of Cyber Security, Security Operations Center will be happy to facilitate this exercise with a workgroup from your agency upon request to the WaTech Service Desk at 360-753-2454.
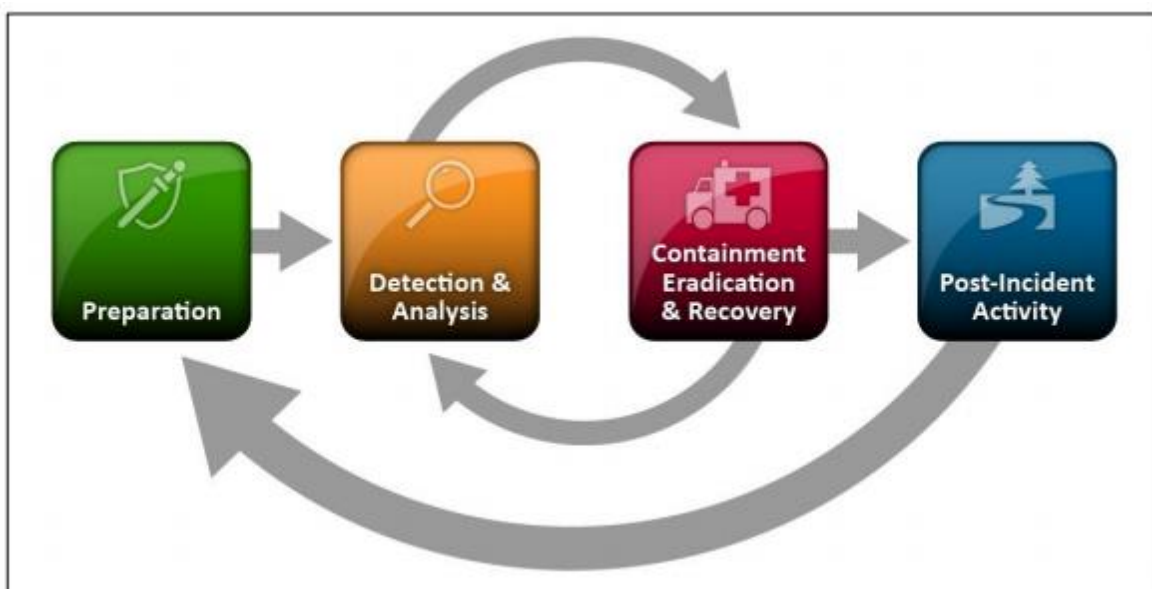
So the new year is off to a rough start, seems that some protesters are incredibly upset that the state refuses to recognize "Squirrel Appreciation Day" and have taken matters into their own hand by occupying one of your organization's buildings. Fortunately, they did this over the weekend so there weren't many employees in the office when it happened. The ones that were there were safely escorted out. The protesters have barricaded themselves in and have bought ample supplies so this might be a long stand-off.

How do you respond?
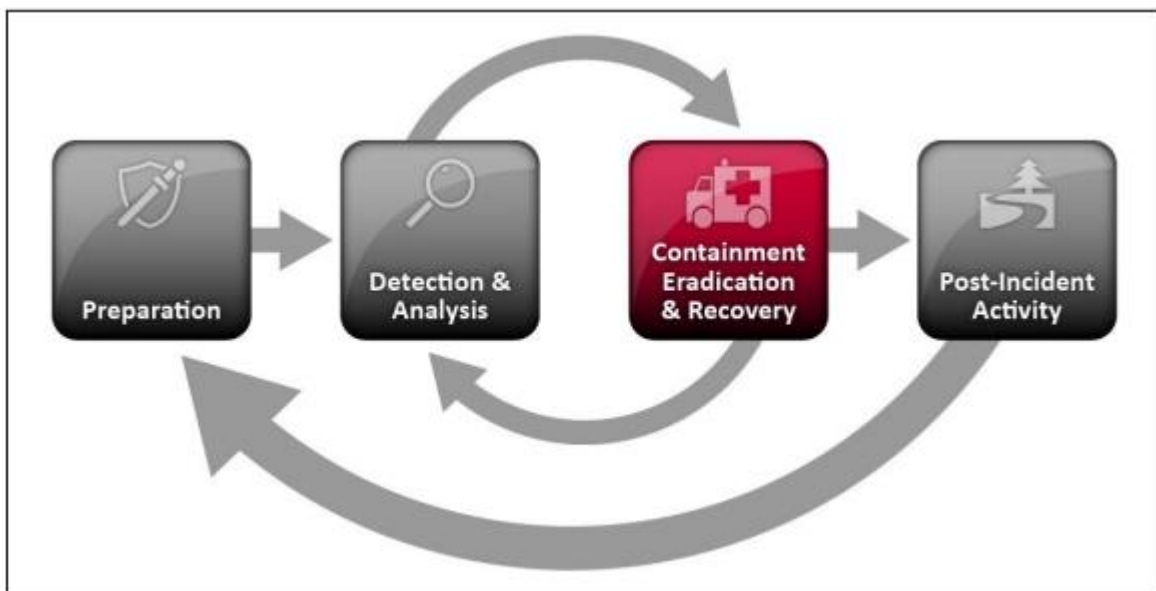
- Who would you contact when you first hear about it?
    - Who should they contact?
- How can you inform employees not to come in to the office?
- At what point do you activate your business continuity plan?
- What kind of backup facilities do you have?
- Who is the lead for recovery efforts?
- How do you communicate the events to senior management?
- Who is responsible for managing public relations?
    - How do you coordinate with this person?
- How can you maintain your critical services without that building?
    - Which services rely upon the impacted infrastructure?
- After the incident is resolved, how do you improve your response plan?

ITEMS TO REPORT

- Did communications flow as expected? If not, why?
- Were processes and procedures followed?
- Were there any surprises?
- How well did the exercise work for your organization?
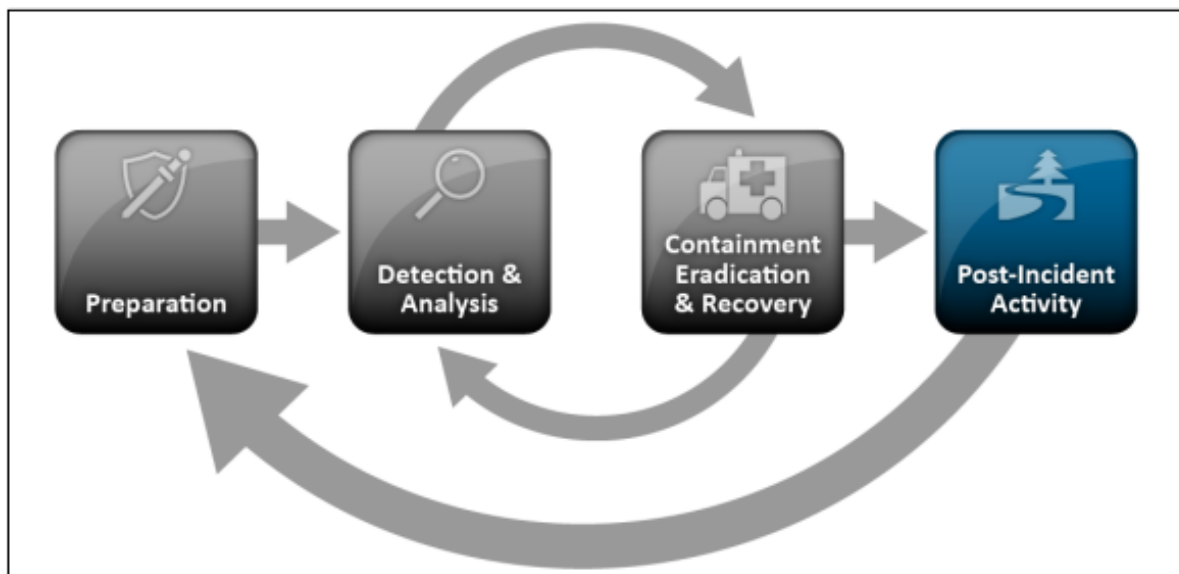
CONTACT US

The State Office of Cyber Security SOC forms a focal point for the efficient reporting, containment, and recovery of security incidents.

To report a cyber-incident, contact the WaTech Service Desk at (360) 753-2454 / 1-888-241-7597.

For general questions, send us an email at soc@watech.wa.gov.

For more information, visit our site at: http://www.soc.wa.gov.

The State Office of Cyber Security, Security Operations Center (SOC) is an active member with the Multi-State Information Sharing and Analysis Center (MS-ISAC) which has been designated by the US Department of Homeland Security (DHS) as the key resource for cyber threat prevention, protection, response and recovery for the nation's state, local, territorial and tribal (SLTT) governments. Through this relationship, the State Office of Cyber Security SOC is able to leverage resources available from MS-ISAC of malware analysis, reverse engineering, log analysis, and forensics analysis in a cyber incident.

The mission of the State Office of Cyber Security SOC is to provide centralized information sharing, monitoring, and analysis of Washington State's security posture. The promotion of cyber security education and awareness to end users is critical to maintenance of a strong security posture of the Washington State network.

SECURITY OPERATIONS